

§314.3 Standards for safeguarding customer information.

(a) *Information security program.* You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in §314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) *Objectives.* The objectives of section 501(b) of the Act, and of this part, are to:

- (1) Insure the security and confidentiality of customer information;
- (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and
- (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

§314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

- (a) Designate an employee or employees to coordinate your information security program.
- (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:
 - (1) Employee training and management;
 - (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

§314.5 Effective date.

(a) Each financial institution subject to the Commission's jurisdiction must implement an information security program pursuant to this part no later than May 23, 2003.

(b) Two-year grandfathering of service contracts. Until May 24, 2004, a contract you have entered into with a non-affiliated third party to perform services for you or functions on your behalf satisfies the provisions of §314.4(d), even if the contract does not include a requirement that the service provider maintain appropriate safeguards, as long as you entered into the contract not later than June 24, 2002.

PART 315—CONTACT LENS RULE

Sec.

315.1 Scope of regulations in this part.

315.2 Definitions.

315.3 Availability of contact lens prescriptions to patients.

315.4 Limits on requiring immediate payment.

315.5 Prescriber verification.

315.6 Expiration of contact lens prescriptions.